UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/524,057	12/29/2005	Tai Pang Chen	212/688US	4440

23371 7590 02/04/2009

CROCKETT & CROCKETT, P.C.
26020 ACERO
SUITE 200
MISSION VIEJO, CA 92691

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
02/04/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/524,057	CHEN ET AL.	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-25 and 27-61* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-25 and 27-61* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAIL ACTION

1. This action is in response to Amendment filed November 7, 2008.

2. Claims 1, 2, 3, 5, 7, 24, 25, 27, 57, 60 and 61 are amended. Claims 4, 6, 26 and 28 are cancelled. Claims 1, 2, 3, 5, 7 - 25, 27 and 29 - 61 are pending.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims 1-3, 5, 7-25, 27, and 29-37 are rejected under 35 U.S.C. 102(e) as being anticipated by Hamid (US Patent No. 2003/0223624).

3. As to claim 1, Hamid teaches a method of authenticating a user according to a biometrics parameter of the user presented at an authentication device on a user-presented device on which is stored a biometrics identification template (i.e., fingerprint template) divided into a secure portion (e.g., private portion) and an open portion (e.g., public portion) [par. 27], the method comprising:

transmitting to a client terminal (i.e., smart card reader interface) data derived from said user biometrics parameter at the authentication device [par. 27], wherein the open portion (e.g., public portion) is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template [par. 27];

transmitting from a user-presented device (i.e., smart card) to the client terminal only the open portion (e.g., public portion) of the said biometrics identification template held on the user-presented device (e.g., smart card) (i.e., ... Hamid teaches transmitting from a smart card a public portion to a host computer [par. 27], a open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template and user-presented device (e.g., ... teaches providing a public portion from a smart card for which is preprocessed registered biometric data [par. 26-27]).

at the client terminal (e.g., host processor) implementing a first stage of an biometric identity authentication process between said derived data and said

open portion to produce intermediate results and transmitting the intermediate results of said biometric authentication process to the user-presented device (i.e., ... teaches a host processor align sensed image with portion of fingerprint received. Extracting the aligned image and creating a image portion [26, 27, fig. 3]), wherein said intermediate results (e.g., image portion) comprise parameters for alignment of said derived data and said biometric identification template (i.e., ... teaches providing a image portion extracted from an aligned image from which a derived private portion was constructed [par. 27]);

and at the user-presented device (i.e., smart card) implementing a second stage of the biometric identity authentication process to complete the biometric identity authentication process using said intermediate results and issuing a biometric authentication result based thereon (e.g., ... teaches a smart card comparing a image portion with a private portion [29, fig. 3]).

4. As to claim 2, Hamid teaches a method of registration of a user according to a biometrics parameter of the user presented at an authentication device [par. 26], the method comprising;

transmitting to an authorized client terminal) data said user biometrics parameter obtained at the authentication device [par. 26];

at the authorized client terminal, dividing the biometrics identification template computed into secure portion and open portion [par. 26], a open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises

parameters of a predetermined number of unique features of the template (i.e., … teaches providing a public portion from a smart card for which is preprocessed registered biometric data [par. 26-27];

transmitting from the authorized client terminal (e.g., imaging device), to a user-presented device both the open portion and the secure portion of a biometrics identification template [par. 26], storing the said template consisting of open and secure portions on the user- presented device [par. 26].

5. As to claim 3, Hamid teaches a method where the secure portion of the biometrics identification template is the portion containing data unauthorized modification of which may cause an impostor to be incorrectly authenticated as a genuine user (i.e., Burger teaches user biometric characteristics stored on a portable standalone device [fig. 1]).

6. As to claim 4, Cancelled.

7. As to claim 5, Hamid teaches a method where the biometrics parameter is a Fingerprint (103, 104, fig. 4).

8. As to claim 6, Cancelled.

9. As to claim 7, Hamid teaches a method where the first stage of said biometric identity authentication process implemented at the client terminal

comprises locating unique features using the data derived from the user biometrics parameter and aligning them with said predetermined number of unique features from the identification template held on the user-presented device (106, fig. 4).

10. As to claim 8, Hamid teaches a method where the second stage of the said identity authentication process implemented on the user-presented device (i.e., smart card) is implemented using a local executable matching program (i.e., application) stored on the device (109, 110, fig, 4).

11. As to claim 9, Hamid teaches a method where the first stage of the identity authentication process implemented at the client terminal is implemented using a client executable matching program (106, 107, fig. 4).

13. As to claim 10, Hamid teaches a method where the client executable matching program is stored on the user-presented device (i.e., smart card) or the authentication device and is transmitted to the client terminal at the time of authentication [par. 23].

14. As to claim 11, Hamid teaches a method where the client executable matching program (i.e., biometric template) is downloaded by the client terminal from a remote memory (i.e., smart card) at the time of authentication [par. 23].

12. As to claim 12, Hamid teaches a method where the authentication result is used to authenticate a user for authorizing a secure transaction [par. 25].

13. As to claim 13, Hamid teaches a method where the secure transaction is controlled by an executable transaction program stored on the user-presented device [par. 64].

15. As to claim 14, Hamid teaches a method where when the authentication result indicates an adequate match, a first security access check key (e.g., image portion) is constructed including the authentication result [26, fig. 3]

16. As to claim 15, Hamid teaches a method where a second security access check key is requested and compared with the first security access key (e.g., image portion), the result of said comparison being used to enable the executable transaction program if it yields a positive authentication result [28, 29, fig. 3].

17. As to claim 16, Hamid teaches a method where the second security access check key (e.g., image portion) is issued from a security server [28, fig. 3].

18. As to claim 17, Hamid teaches a method where the first and second security access check keys each include a unique identification number [24, fig. 3].

19. As to claim 18, Hamid teaches a method where the unique identification number contains a number obtained from a mathematical operation on a randomly generated number and the authentication result [par. 48].

20. As to claim 19, Hamid teaches a method where the randomly generated number changes at each time the number is used [par. 55].

21. As to claim 20, Hamid teaches a method where the changing random number is tracked by dividing the number into two portions, a first portion to be used as the current random number and a second portion to be used as the next random number [par. 47.

14. As to claim 21, Hamid teaches a method where the unique identification number contains a number that is remembered by the user [par. 27].

22. As to claim 22, Hamid teaches a method where more than one authentication methods can be used to obtain the authentication result, each being incorporated into the unique identification number (par. 27).

15. As to claim 23, Hamid teaches a method where the access is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained from the unique identification number (i.e., ... teaches a multiple security level using PIN and biometric authentication [par. 27]).

16. As to claim 24, Hamid teaches a system for authenticating a user according to a biometrics parameter of the user, the system comprising:

a user-presented device (i.e., smart card) on which is stored a biometrics identification template divided into a secure portion and an open portion [par. 26],

where only said open portion can be transmitted out of the said device;

an authentication device (i.e., smart card reader interface) operable to read biometrics data derived from a user [25, fig. 3], where only said open portion is the portion containing data unauthorized modification of which may not cause an impostor to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template (i.e., ... teaches providing a public portion from a smart card for which is preprocessed registered biometric data [par. 26-27]),

an authentication device operable to read biometric data derived from a user [par. 27], and comprising means for communicating with the user-presented device and a client terminal (par. 23)

a client terminal arranged to receive the said open portion of the biometrics identification template held on the user-presented device (i.e., smart

card) and the biometrics data derived from the user, and comprising a client processor operable to implement a first stage of biometric identity authentication process between said derived data and said open portion to produce intermediate results [par. 27], and to transmit the intermediate results of said biometric identity authentication process to the user-presented device [28, fig. 3],

wherein said intermediate results (e.g., image portion) comprise parameters for alignment of said derived data and said biometric identification template (i.e., ... teaches a providing a image portion extracted from an aligned image from which a derived private portion was constructed [par. 27]);

and wherein the user-presented device (i.e., smart card) comprises a device processor operable to implement a second stage of the biometric identity authentication process to complete the biometric identity authentication process using said intermediate results and to issue a biometric authentication result based thereon (to provide a smart card biometric authentication capability [col. 7, lines 60-67]).

17. As to claim 25, Hamid teaches a system where the secure portion of the biometrics identification template is the portion containing data unauthorized modification of which may cause the system to incorrectly authenticate an impostor as a genuine user [par. 23]

18. As to claim 26, Cancelled

19. As to claim 27, Hamid teaches a system where the biometrics parameter is a fingerprint, and where the authentication device includes a fingerprint Sensor (par. 23).

20. As to claim 28, Cancelled.

21. As to claim 29, Hamid teaches a system where the user-presented device (i.e., smart card) comprises a memory (i.e., micro chip) in which is stored a local executable matching program (i.e., application) for implementing the second stage of the matching process [par. 64].

22. As to claim 30, Hamid teaches a system where the memory on the user-presented device stores a client executable matching program which is transmitted to the client processor to implement the first stage of the matching process (par. 23).

23. As to claim 31, Hamid teaches a system which comprises a security server connected to the client terminal [par. 64].

23. As to claim 32, Hamid, teaches a system where the security server (i.e., host processor) holds a client executable matching program for implementing the first stage of the matching process [par. 23].

24. As to claim 33, Hamid teaches a system where the security server holds a security access check key requestable (e.g., biometric sample) by the client terminal for enabling a transaction [par. 64].

24. As to claim 34, Hamid teaches a system which comprises a transaction server arranged to implement secure transactions and which is in communication with the client terminal so that the authentication result is usable to authenticate a user for authorizing a secure transaction [par. 25].

25. As to claim 35, Hamid teaches a system where the user-presented device stores an executable transaction program (i.e., biometric data) for controlling the secure transaction (par. 64).

26. As to claim 36, Hamid teaches a system where more than one authentication methods can be used to obtain the authentication result (par. 27)

27. As to claim 37, Hamid teaches a system where the access to the transaction server is divided into several levels and wherein the level of access granted to a user is dependent on the confidence level of positive identity obtained based on the results from the various authentication methods used (par. 27).

28. Claims 38-43, 45-61 are rejected under 35 U.S.C. 102(e) as being anticipated by Studd et al. (US Patent Publication No. 2004/0122774 and Studd hereinafter).

29. As to claim 38, Studd teaches a method of executing an operation using first and second processors, the method comprising:

storing in the first processor a first task table containing a plurality of process names (i.e., mobile device application) with associated process identifiers, each associated with a process locator (i.e., Studd teaches a request for a list of mobile device application from mobile to device for which said mobile device application will be stored and executed [par. 51]);

storing in the second processor a second task table containing said of process names and process identifiers (i.e., Studd teaches a mobile device containing list mobile device application [par. 51]);

identifying at the second processor a process to be executed and issuing a request to the first processor to execute said process (i.e., Studd teaches identifying a mobile application to execute [par. 51 - par. 53]);

locating said process using the process locator and executing said process at the first processor to generate a result [par. 51 - par. 53]; and returning the result to the second processor [par. 51 - par. 53].

30. As to claim 39, Studd teaches a method where said process names (i.e., identifiers) include object names associated with respective object identifiers [par. 51, lines 7-10].

31. As to claim 40, Studd teaches a method where each object has associated therewith a plurality of functions (i.e., mobile device application) each identified by function names and associated function identifiers in the first and second task tables (par. 51).

32. As to claim 41, Studd teaches a method where the process locator identifies (i.e., identifier) the starting address of a process in a program memory (par. 51, lines 7-10).

33. As to claim 42, Studd teaches a method where the second processor has significantly less processing power than the first processor (par. 29, lines 8-11).

34. As to claim 43, Studd teaches a method where the second processor is arranged to execute locally processes requiring less processing power than those executed by the first processor [fig. 5].

35. As to claim 45, Studd teaches a method where there are a plurality of second processors in communication with a single first processor, each second

processor holding a respective task table, and the first processor holding a first task table (i.e., mobile device application) including all processes identified by the task tables of the second processors (i.e., Studd teaches a mobile device with a list of mobile device applications [par. 50- par. 53]).

36. As to claim 46, Studd teaches a method where a client bridge (i.e., predetermine mechanism) is connected between the first and second processors, the client bridge (i.e., predetermine mechanism) conveying said requests from the second processor to the first processor and returning the results from the first processor to the second processor (par. 100).

37. As to claim 47, Studd teaches a method where the first processor is a client terminal and the second processor is embedded on a secure portable computing and data storage platform [404, fig. 4]

38. As to claim 48, Studd teaches a method where there are a plurality of first processors connected (i.e., multiple processors) via a client bridge to one or more second processor and arranged to implement different subsets of the processes in the task table of the second processor [par. 29, lines 7-11].

39. As to claim 49, Studd teaches a processing system comprising:
a first processor in which is stored a first task table containing a plurality of process names and process identifiers, each associated with a process locator

(i.e., Studd teaches a request for a list of mobile device application from mobile to device for which said mobile device application will be stored and executed [par. 51]);

a second processor in which is stored a second task table containing said process names with associated process identifiers (i.e., Studd teaches a mobile device containing list mobile device application [par. 51]);

the second processor including a distributed object execution manager for identifying a process to be executed and issuing a request to the first processor to execute said process (i.e., Studd teaches identifying a mobile application to execute [par. 51 - par. 53]);

and the first processor including a client distributed object execution manager for controlling the execution of said processes at the first processor, the results of execution of the processes implemented at the first processor being returned to the second processor [par. 51 - par. 53].

40. As to claim 50, Studd teaches a processing system where the first processor includes a client manager (i.e., input/output controller hub) for handling communications between the first and second processors (par. 31).

41. As to claim 51, Studd teaches a system where the first processor includes an execution manager (i.e., framework application services unit) for handling the execution of processes (i.e., mobile device application) [par. 51 - par. 53].

42. As to claim 52, Studd teaches a system where the first processor comprises a program store for holding said processes, the process locator (i.e., identifier) being used to identify the location of said processes in the program store [par. 51].

43. As to claim 53, Studd teaches a system where the second processor includes a remote device manager for transmitting said requests to the first processor [fig. 4].

44. As to claim 54, Studd teaches a system where the second processor comprises a stack for holding results returned to it from the first processor (par. 61).

45. As to claim 55, Studd teaches a system according where the second processor includes a program store for holding said processes (par. 51).

46. As to claim 56, Studd teaches a system where the first processor comprises a client terminal (fig. 4).

47. As to claim 57, Studd teaches a system which comprises a plurality of first processors, the system further comprising a client bridge (i.e., predetermine mechanism) for handling communications between the first processors and the second processor [par. 100].

48. As to claim 58, Studd teaches a system where each first processor comprises a server (par. 100, lines 6-9).

49. As to claim 59, Studd teaches a system where the client bridge includes a network execution manager (i.e., input/output controller hub) for transmitting requests from the second processor to the appropriate one of the first processors, based on a processor identifier in the request [par. 31, lines 1-8].

50. As to claim 60, Studd teaches a system comprising a plurality of second processors and a client bridge (i.e., predetermine mechanism) for connecting said second processors to said first processor [par. 100, lines 1-9].

51. As to claim 61, Studd teaches a system where the second or each second processor is embedded on a respective portable secure computing and data storage platform such as smart card [par. 404, fig. 4].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

52. Claim 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Studd in view of Hamid.

53. As to claim 44, the system disclose by Studd teaches substantial features of the claim invention (discussed above) it fails to disclose:

A method where the operation being executed is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor (claim 44).

However, these features are well known in the art and would have been an obvious modification of the system disclosed by Studd as introduced by Hamid. Hamid discloses:

A method where the operation being executed is a fingerprint-matching algorithm comprising a base minutiae finding process executed by the first processor and a minutiae matching process executed by the second processor (claim 44) (to provide a fingerprint minutiae matching algorithm [col. 7, lines 20-51]).

Therefore, given the teachings of Hamid, a person having ordinary skill in the art at the time of the invention would have recognized the desirability and advantage of modifying Studd by employing the well known features of a fingerprint

matching algorithm disclosed above by Hamid, for which distributed authentication will be enhanced [col. 7, lines 20-51].

Response to Arguments

Applicant's arguments, see Applicant Remarks, filed 11/7/2008, with respect to the rejection(s) of claim(s) Claims 1, 2, 3, 5, 7 - 25, 27 and 29 - 61 have been fully considered and are persuasive. Examiner acknowledges that dependent claims 4-6 are now rolled into independent claim 2 and therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Hamid. Examiner has provided a response to applicant's remarks filed on 11/7/2008 in view of the new rejection set forth in this office action.

Applicant Remarks – Burger Reference – Claims 1-9, 12, and 13

55. Applicant argue, "The method of Burger does not implement a first stage of a biometric identity authentication process at the client terminal and a second stage implemented at the user-presented device. Rather, the entire biometric identity authentication process is implemented at the client terminal. Although Burger teaches a second comparison/authentication of user information between the non-biometric identifier of the smart card and other user data stored remote from the smart card (claim i, Col. 6, ii. 48-51 and Col. 7, ii. 1-44), such a second authentication of non- biometric information is not part of the biometric identity authentication process and is implemented at the client terminal instead of the

user-presented device. Thus, the user-presented device (i.e. the smart card) in Burger is only used for storing. Neither the biometric identity authentication process nor the authentication of non-biometric information is implemented at the user-presented device in Burger'.

Examiner contends the applicant arguments are moot under the new rejection in view Hamid. The teachings of Hamid specifically teaches a two stage biometric authentication between a smart card (e.g., user-presented) and host processor [figure 5].

56. Applicant argues, "Burger also does not teach or suggest that the biometric identification template is divided into a secure portion and an open portion, and that only the open portion of the biometric identification template is transmitted from the user-presented device to the client terminal. Rather, the entire biometric identification template of Burger is transmitted out of the user-presented device (Col. 6, ii. 39-42). The user identification data (Col. 7, ii. 1-5) of Burger which is transmitted out of the secure user-presented device is not biometric data and does not belong to the biometric identification template, and therefore cannot be considered as the open portion of the biometric identification template. Therefore, all the limitations of amended claim 1 are not disclosed in Burger and thus are not anticipated by Burger. This rejection should be withdrawn. Dependent claims 3, 5, 7-9, 12 and 13 depend from amended claim 1 and thus the rejection with respect to the dependent claims should also be withdrawn. Claim 2 as amended, defines a method of registration of a user

according to a biometric parameter of the user. A computed biometric identification template is divided into secure portion and open portion at the authorized client terminal. The open portion contains data unauthorized modification of which may not cause an imposter to be incorrectly authenticated as a genuine user, and comprises parameters of a predetermined number of unique features of the template. Both secure portion and open portion are transmitted to and stored on a user-presented device, wherein the secure portion is only accessible within the user-presented device and not externally. As discussed above, Burger does not disclose the dividing of the biometric identification template into secure portion and open portion at the authorized client terminal, and transmitting and storing both secure portion and open portion of the template on the user-presented device. Therefore, all the limitations of amended claim 2 are not disclosed in Burger and thus are not anticipated by Burger. This rejection should be withdrawn".

Examiner contends the applicant arguments are moot under the new rejection in view Hamid. The teachings of Hamid specifically teaches a two stage biometric authentication between a smart card (e.g., user-presented) and host processor containing a private and public portion biometric template [fig. 5].

Applicant Remarks – Studd Reference – Claims 38 - 43 and 45 - 61

Applicant's arguments with regards to claims 28-43 and 45-61 have been fully considered but they are not persuasive.

57. Applicant argues, "Studd teaches that the mobile device applications are associated with the framework applications, and the framework application associated with the selected mobile device application can be identified (paragraphs [0053]-[0054]). However, Studd does not disclose that the process names and process identifiers in the second task table are those process names and process identifiers in the first task table, and does not disclose that a process locator is used to locate the selected process in the first processor as required by claim 38. Studd does not disclose returning the result in the first processor to the second processor, but discloses receiving data from the second processor (paragraph [0063]). Thus this rejection should be withdrawn. Dependent claims 39-43, 45-48 depend from independent claim 38 and thus the rejection with respect to the dependent claims should also be withdrawn. As discussed above, the apparatus of independent claim 49 which corresponds to the method of claim 38 is not anticipated by Studd and thus the rejection should be withdrawn. Dependent claims 50-61 depend from claim 49 and the rejection of the dependent claims should also be withdrawn".

Examiner contends the subject matter for which applicant is seeking to claim is exemplary inherent to an execution manager in a multi-threaded process computing environment. The tables containing processes (e.g., applications) for which will execute upon the calling of the process identifier are used by an execution manager for the purpose of assigning runtime for each process. Stud teaches such a execution management framework in paragraph 51. With regards

to the applicant's argument of, "Studd does not disclose that the process names and process identifiers in the second task table are those process names and process identifiers in the first task table", Examiner contends this claim element is however suggested in the teaching of Studd, paragraph 52 for which recites determining by identifier the correspondence of a application (e.g., process) too a separate set of applications. Here the teachings of Studd would suggest there exist two sets of processes (e.g., application), for which one set of processes are used for the purpose of corresponding relevancy. With regards to applicant arguments of, "Studd does not disclose returning the result in the first processor to the second processor", Examiner cites paragraph 80 of Studd. The teachings in paragraph 80 specifically teach an authentication result is transmitted between two processors. The transmission is between an authentication device (e.g., smart card) and an authentication server. Those skilled in the art would recognize that the smart card contains a processor and the authentication server contains a processor.

Applicant Remarks – Burger in view of Studd – Claims 14 -17 and 23

Applicant's arguments with respect to claims 14-17 and 23 have been considered but are moot in view of the new ground(s) of rejection.

58. Applicant argues, "Burger does not teach or suggest dividing the biometric identity authentication process into 2 stages, and does not teach or suggest implementing the 2 stages at a client terminal and a user-presented device,

respectively. In addition, Burger does not teach or suggest that the biometric identification template is divided into a secure portion and an open portion, and further that only the open portion of the biometric identification template is transmitted from the user- presented device to the client terminal. Therefore, amended claim 1 is not obvious in light of Burger. Studd does not teach or suggest the missing limitations and thus the Examiner's proposed combination does not render claim 1 obvious. Claims 14 through 17 and 23 depend from claim 1 and thus the rejection with respect to the dependent claims should be withdrawn".

Examiner contends the applicant arguments are moot under the new rejection in view Hamid. The teachings of Hamid specifically teaches a two stage biometric authentication between a smart card (e.g., user-presented) and host processor containing a private and public portion biometric template [fig. 5].

Applicant Remarks – Burger in view of Scheidt – Claims 18- 20

Applicant's arguments with respect to claims 18-20 have been considered but are moot in view of the new ground(s) of rejection.

59. Applicant argues, "As discussed above, amended claim 1 is not obvious in light of Burger. Scheidt does not teach or suggest the missing limitations and thus the Examiner's proposed combination does not render claim 1 obvious. Claims 18 through 20 depend from claim 1 and thus the rejection with respect to the dependent claims should be withdrawn".

Examiner contends the applicant arguments are moot under the new rejection in view Hamid. The teachings of Hamid specifically teaches a two stage biometric authentication between a smart card (e.g., user-presented) and host processor containing a private and public portion biometric template [fig. 5].

Applicant Remarks – Burger in view of Hamid – Claims 10, 11, 24-29 and 30-32

Applicant's arguments with regards to claims 10, 11, 24-29 have been fully considered but they are not persuasive.

60. Applicant argues, "Hamid discloses a method of generating public data that can be used for fingerprint matching. The public data is hashed data in the form of offset locations or alignment locations (Col. 6, 22 ii. 35-38 and Col. 7, ii. 41-43), and is transmitted from a user-presented device (e.g. smartcard) to a client terminal (e.g. host processor) for alignment of a captured fingerprint image. However, the public data in Hamid is hashed offset locations or alignment locations, and is not a portion of the biometric identification template. Therefore,

Hamid does not disclose or suggest dividing the biometric identification template into secure portion and open portion, wherein the open portion contains data unauthorized modification of which may not cause an imposter to be incorrectly authenticated as a genuine user and comprises parameters of a predetermined number of unique features of the template".

Examiner contends Hamid teaches a public portion created using enrollment data from the user [par. 22]. This would suggest to one of ordinary skill in the art that an impostor could not duplicate the public portion or make any modification to it. Also, the teachings of paragraph 26, specifically recite the use of a public and private portion comprising the biometric template.

61. Applicant argues, "Thus Hamid does not provide the missing limitations to render amended claim 1 obvious in light of Burger as discussed above. Thus the rejection of dependent claims i0 and ii should be withdrawn. Independent claim 24 is an amended apparatus claim corresponding to amended method claim i. As discussed above with respect to amended claim i, the Examiner's proposed combination of Burger and Hamid do not teach, suggest or render obvious all the limitations of claim 24 and thus the rejection should be withdrawn. Dependent claims 25 through 29 and 30 depend from amended claim 24 and thus the rejection with respect to the dependent claims should also be withdrawn. The Examiner has not provided any motivation to make the proposed combination of Burger and Hamid. As Hamid specifically disclaims the transmission of any biometric data (Background of the Invention) the Examiner's proposed

combination of Burger with Hamid must find an explicit motivation to combine the references sufficient to overcome the teaching of Hamid against the transmission of biometric data. No such motivation is provided and thus the rejections based on this proposed combination should be withdrawn".

Examiner contends the applicant arguments are moot under the new rejection in view Hamid. The teachings of Hamid specifically teach a two stage biometric authentication between a smart card (e.g., user-presented) and host processor containing a private and public portion biometric template [fig. 5].

Applicant Remarks – Burger in view of Stud and further in view of Hamid – Claims 21 and 22

Applicant's arguments with respect to claims 21 and 22 have been considered but are moot in view of the new ground(s) of rejection.

62. Applicant argues, "Claims 21 and 22 stand rejected under 35 U.S.C §103(a) as unpatentable over Burger, in view of Studd and Hamid. As discussed above, the proposed combination does not teach, suggest or render obvious the limitations of independent claim i. Claims 21 and 22 depend from claim 1 and thus the rejection with respect to these claims should be withdrawn. The Examiner has not provided any motivation to combine Hamid with Burger and Studd. As discussed, the explicit disclaimer of Hamid to the transmission of biometric date renders the Examiner's proposed combination impossible absent explicit motivation to combine".

Examiner contends the applicant arguments are moot under the new rejection in view Hamid. The teachings of Hamid specifically teaches a two stage biometric authentication between a smart card (e.g., user-presented) and host processor containing a private and public portion biometric template [fig. 5].

Applicant Remarks – Burger in view of Hamid – Claims 33 - 37

Applicant's arguments with respect to claims 33-37 have been considered but are moot in view of the new ground(s) of rejection.

63. Applicant argues, "This rejection should be withdrawn. Claims 33 through 37 stand rejected under 35 U.S.C §103(a) as unpatentable over Burger, in view of Hamid and Studd. As discussed above, the proposed combination does not teach, suggest or render obvious the limitations of amended independent claim

24. Claims 33 through 37 depend from amended claim 24 and thus the rejection with respect to these claims should be withdrawn. The Examiner has not provided any motivation to combine Hamid with Burger and Studd. As discussed, the explicit disclaimer of Hamid to the transmission of biometric date renders the Examiner's proposed combination impossible absent explicit motivation to combine. This rejection should be withdrawn".

Examiner contends the applicant arguments are moot under the new rejection in view Hamid. The teachings of Hamid specifically teaches a two stage biometric authentication between a smart card (e.g., user-presented) and host processor containing a private and public portion biometric template [fig. 5].

Applicant Remarks – Studd in view of Hamid – Claim 44

Applicant's arguments with regards to claim 44 have been fully considered but they are not persuasive.

64. Applicant argues, " Claim 44 stands rejected under 35 U.S.C §103(a) as unpatentable over Studd in view of Hamid. As explained above, Studd does not teach, suggest or render obvious storing a second task table containing the process names and process identifiers which are those process names and process identifiers in the first task table, and does not teach, suggest or render obvious that a process locator is used to locate the selected process in the first processor as defined in claim 38. By storing the same process names and

process identifiers in the first processor and the second processor and storing the process locator to locate the selected process in the first processor, the second processor of claim 38 simply issues a request to the first processor such that the first processor locates the selected process using the process locator and executes the selected process. Hamid does not teach, suggest or render obvious the method of executing an operation using first and second processors as claimed in claim 38. In particular, Hamid does not disclose the first task table and the second task table, and does not disclose or suggest locating a selected process using a process locator. In view of the above, Studd and Hamid, either alone or in combination, do not teach, suggest or render obvious the limitations of claim 38. Therefore, the rejections of claim 38 and of its dependent claims 39-48 should be withdrawn."

Examiner contends Hamid use of a host processor and a smart card containing a processor suggests a first and second processor environment [par. 23 & 64]. Applicants reciting of a first and second task table could be recognized by one of ordinary skill the art as suggested by each processor will contain a process manager that will allocate processing time for each biometric authentication process containing a process id as necessitated by communication exchange between the two processors.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435